

FILED 05 JUL '18 08:54 USDC-ORE

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*792 Barrett Avenue, Eugene, OR, a 1997 Honda
Passport, and the person of Eamonn Isaiah
Martinez-Wenzl, as described in Attachment A

Case No. 6:18-mc- 575

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
792 Barrett Avenue, Eugene, OR, a 1997 Honda Passport, and the person of Eamonn Isaiah Martinez-Wenzl, as described in Attachment A,

located in the _____ District of _____ Oregon _____, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2113(a)

Offense Description
Bank Robbery

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn on 7.3.18 at 3:36 p.m.
pursuant to Rules 4.1 and 41(d)(3)

Applicant's signature

Miguel A. Perez, Special Agent FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: July 3, 2018

City and state: Portland, Oregon

J. V. Acosta

Judge's signature

John V. Acosta, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Premises, Person, and Vehicles to Be Searched

1. Premises: 792 Barrett Avenue, Eugene, Oregon 97404

The property to be searched is 792 Barrett Avenue, Eugene, Oregon 97404, further described as a single family home yellow/tan in color, with a brown roof, and with several large trees in the front yard. Below is a photograph of the premises.



2. Vehicle: 1997 Honda Passport

The vehicle to be search is a 1997 Honda Passport with Oregon license plate 242CQF, further described as an SUV dark grey in color, with a cargo box on top, and a spare tire attached to the tailgate. Below is a photograph of the vehicle.



3. Person: Eamonn Isaiah Martinez-Wenzl

The person to be search is Eamonn Isaiah Martinez-Wenzl, DOB 8/20/1981, who stands approximately 5'11" and weighs approximately 220 pounds. Below is a photograph of Eamonn Isaiah Martinez-Wenzl.



ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises, vehicle, and person identified in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2113(a) (Bank Robbery). The items to be seized cover the period of March 1, 2018, through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:
 - a. Clothing to include baseball caps, skull caps, sunglasses, shirts, sweaters, blue jeans, and shoes;
 - b. Over the shoulder satchel bags;
 - c. Banking deposit bags;
 - d. Any “fake” beard(s) and items used in the application of the beard(s);
 - e. Any phones or electronic devices;
 - f. Any receipts for purchases which may indicate dates and times of purchase and method of payment used;
 - g. Any currency;
 - h. Papers, records, documents, files, notes, memos, mail, or other materials representing residency, ownership, occupancy, dominion, or control of the premises referenced above and described in Attachment A;
 - i. Papers, records, documents, files, notes, memos, mail, or other materials

representing residency, ownership, occupancy, dominion, or control of the vehicle referenced above and described in Attachment A; and

- j. Books, records, receipts, notes, ledgers, and other documents relating to bank institutions.

2. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

- a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs,

and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity,

including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to

examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF MIGUEL A. PEREZ

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, Miguel A. Perez, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since January 2015. I am currently assigned to the Portland Division at the Eugene, Oregon Resident Agency. During my training in the FBI Academy in Quantico, Virginia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment Searches and probable cause. My responsibilities include the investigation of federal criminal offenses, to include Title 18, United States Code, Section 2113(a) (Bank Robbery).

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 792 Barrett Avenue, Eugene, Oregon 97404 (hereinafter "Premises"), a 1997 Honda Passport with Oregon license plate 242CQF (the "Vehicle"), and the person Eamonn Isaiah Martinez-Wenzl aka Martinez Wenzel (Martinez-Wenzl) as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2113(a) (Bank Robbery). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at the Premises, Vehicle, and on Martinez-Wenzl.

////

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, United States Code, Section 2113(a)(Bank Robbery) provides that whoever, by force and violence, or by intimidation, takes, or attempts to take, from the person or presence of another, or obtains or attempts to obtain by extortion any property or money or any other thing of value belonging to, or in the care, custody, control, management, or possession of, any bank, credit union, or any savings and loan association; or whoever enters or attempts to enter any bank, credit union, or any savings and loan association, or any building used in whole or in part as a bank, credit union, or as a savings and loan association, with intent to commit in such bank, credit union, or in such savings and loan association, or building, or part thereof, so used, any felony affecting such bank, credit union, or such savings and loan association and in violation of any statute of the United States, or any larceny—shall be fined under this title or imprisoned not more than twenty years, or both.

Statement of Probable Cause¹

¹ Based on my training and experience, I use the following technical terms to convey the following meanings:

5. Law enforcement is investigating Eamonn Isaiah Martinez-Wenzl (Martinez-Wenzl), date of birth XX/XX/1981, and others as part of its investigation into the robbery of multiple banks in the Eugene, Oregon area.

March 30, 2018 Robbery

6. On March 30, 2018, at approximately 6:08 p.m., the Chase Bank located inside Fred Meyer at 3333 W. 11th Ave, Eugene, Oregon, was robbed by a white male wearing a black baseball cap and headphones with sunglasses and a beard according to bank surveillance videos. The robber presented a demand note that said he had a weapon. The note was taped to a zippered bank deposit type bag. The robber told the victim teller, "Give me all your money in your drawer or everyone will get holes." The robber made his getaway with the note and the money on a bicycle. Chase Bank suffered a loss of \$3,760.00, which was then and there insured by the Federal Deposit Insurance Corporation (FDIC).

a. *IP address.* The Internet Protocol address (or simply "IP address") is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

April 24, 2018 Robbery

7. On April 24, 2018, at approximately 6:28 p.m., the Chase Bank located inside Fred Meyer at 60 Division Avenue, Eugene, Oregon, was robbed by a white male. According to bank surveillance videos, he wore a grey skull cap, sunglasses, and a checkered shirt and appeared older and heavier than the robber of the March 30, 2018, robbery. However, this robber similarly presented a demand note produced from within a zippered bank deposit type bag to a bank teller. The note read, "Give me all your bills or I will start shooting holes in everyone." The robber carried an over-the-shoulder satchel in which he placed the money and left with the note and the money on a bicycle. Chase Bank suffered a loss of \$2,128.00, which was then and there insured by the FDIC.

May 14, 2018 Robbery

8. On May 14, 2018, at approximately 4:52 p.m., the U.S. Bank located inside Albertson's at 4740 Royal Avenue, Eugene, Oregon, was robbed by a white male who looked similar to the robber in the April 24, 2018, robbery. According to bank surveillance videos, the male wore a skull cap, checkered shirt, sunglasses and had a goatee. The robber presented a note written on a check to a bank teller. A sticker covered the registered owner printed on the check. Written on the amount line were words to the effect of "Give me all the money and put it in the bag." Written in the memo section was, "Do it or draw attention and you all will get hurt." Like with prior robberies, the robber had a zippered bank deposit type bag and an over-the-shoulder satchel in which he placed the money. The robber made his getaway with the note and the money. It is currently unknown how the robber left the scene. U.S. Bank suffered a loss of \$1,292.00, which was then and there insured by the FDIC.

June 5, 2018 Potential Bank Robbery

9. On June 5, 2018, at approximately 6:00 p.m., a suspicious person entered and exited the Fred Meyer on 60 Division Avenue, which was robbed on April 24, 2018. The surveillance videos from that evening captured the man entering the grocery entrance, at the east side of the store. While the subject looks to be a different person from the individuals who robbed the previously mentioned banks, he has similar attire and accessories. The male was wearing a black skull cap, sunglasses, a red long sleeve shirt, had a black goatee, dark pants, and an over-the-shoulder satchel type bag. The satchel looked similar to the one used by the bank robber in the May 14, 2018, robbery.

10. The subject immediately walked towards the Chase Bank. When the subject got to the entrance to the Chase Bank, he stopped, and looked inside and then walked away in the opposite way he came into the store and exited out the apparel entrance. Since the last robbery, Chase Bank hired a security guard to be at the location who was working at the time and was inside the bank. The subject at no time did any shopping, but simply walked in, walked to the bank, stopped, looked inside and then exited and got on his bicycle and left the area. The following are images of the subject from the surveillance video:



11. Outside the Fred Meyer store, a Loss Prevention employee for the store observed the subject walking away from the Chase Bank located inside the store. The employee was aware of the recent robbery at the same Chase Bank and was immediately suspicious of the way the subject was dressed for the weather so he followed him. The subject walked out of the store via the apparel exit and walked along the building towards the grocery entrance. The subject then grabbed a bicycle that was left by the flowers on the outside of the grocery entrance and rode across Division Avenue to the parking lot of a second hand store. The March 30, 2018, robber also departed by bicycle. The subject picked up his bicycle and placed it in the back of the Vehicle, an SUV that had no hood. After loading the bicycle in the Vehicle, the subject drove out of the lot.

12. Martinez-Wenzl is not listed as a register owner of the Vehicle. However, as of June 13, 2018, the vehicle registration history indicated it had been sold and had not yet been registered by the new owner. However, law enforcement has connected Martinez-Wenzl to the Vehicle. On May 16, 2018, law enforcement approached Martinez-Wenzl who was sitting in the Vehicle parked in the parking lot at 6898 Main Street in Springfield, Oregon, after reports from a concerned citizen that someone had been sitting in the Vehicle for hours. Law enforcement found Martinez-Wenzl with small quantities of methamphetamine, heroin, an S&W 9MM handgun, and an SKS rifle was located under property in the Vehicle. Martinez-Wenzl was arrested for possession of methamphetamine and heroin along with an outstanding warrant.

13. Martinez-Wenzl's Oregon driver's license lists the Premises as his residence. Additionally, Martinez-Wenzl appears similar to the person in the June 5, 2018, surveillance video based on his Oregon driver's license photo.

June 28, 2018 Robbery

14. On June 28, 2018, at approximately 3:26 p.m., the U.S. Bank located inside the Albertson's Grocery Store at 1675 W. 18th Avenue, Eugene, Oregon, was robbed by a lone white male who looked similar to the suspicious male from the June 5, 2018, incident at the Fred Meyer. The bank robber was wearing a gray skull cap, a white long sleeve button down shirt, sunglasses, and has a black goatee. The teller believed the goatee was fake. The robber presented a note written on a check. The note stated in effect, "Give me the money, quickly and quietly. Place the money in the bag". The note also said he had a gun and not to alert anyone or set off the alarm. The teller only focused on the written portion of the check and did not notice a name on the check. The robber had a maroon or brown zippered bank deposit bag. The money was placed in the bank bag and it was placed in an over-the-shoulder satchel. He exited the store but it is unknown how he left the area. The U.S. Bank suffered a loss of \$439.00, which was then and there insured by the FDIC.

15. Surveillance video from the robbery captured images of the bank robbery. The following is an image of the bank robber taken by the surveillance video:



16. Comparing the videos from the June 5, 2018, potential bank robbery and the Oregon license photo of Martinez-Wenzl to the suspect in this robbery, it appears to be the same person. Based on the above, I have probable cause to believe and do believe that Martinez-Wenzl robbed a U.S. Bank on June 28, 2018, and may be part of a crew conducting bank robberies in the Eugene area. I believe that he used the Vehicle in furtherance of this crime as well. On June 15, 2018, law enforcement observed the Vehicle parked at the Premises.

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, Vehicle, and person of Martinez-Wenzl, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know: that bank robbers, and others involved in criminal activity, will plan, coordinate, and carry out unlawful activity with the use of cell phones. The bank robberies being investigated appear to have been conducted in a similar manner and by the same person/persons. The description of the robbers has varied slightly and therefore could have been executed by Martinez-Wenzl and other individuals. A cell phone, including location of the phones itself, can evidence the crime.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital

device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

21. Because several people may share the Premises as a residence, it is possible that the Premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

22. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

23. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

24. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

25. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

26. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

27. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

28. Based on the foregoing, I have probable cause to believe, and I do believe, that Eamonn Isaiah Martinez-Wenzl committed Bank Robbery in violation of Title 18, United States Code, Section 2113(a), and that contraband, evidence, and instrumentalities of that offense, as described above and in Attachment B, are presently located at 792 Barrett Avenue, Eugene, Oregon 97404, in the 1997 Honda Passport with Oregon license plate 242CQF, and on the person Eamonn Isaiah Martinez-Wenzl aka Martinez Wenzel, which are described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Premises, Vehicle, and person described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

29. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Joseph Huynh, and AUSA Huynh advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

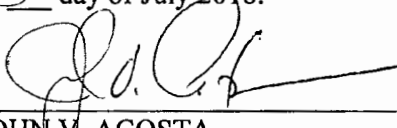
Request for Sealing

30. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

*Sworn 7.3.18 @ 3:36 p.m. pursuant
to Rule 4.1 and 41(d)(3). JAC*

Miguel A. Perez
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me this 3rd day of July 2018.



JOHN V. ACOSTA
United States Magistrate Judge